Le service web Cisco VPN victime de backdoor

Les produits réseau Cisco sont de nouveau sous le feu des attaques. Cette fois, c'est le service Web VPN qui fait parler de lui. La société de sécurité Volexity a annoncé, la semaine dernière, avoir constaté des attaques sur Cisco Clientless SSL VPN. Ce service permet aux clients utilisateurs des appliances Adaptive Security (ASA) de l'équipementier d'accéder, via un portail web, au réseau interne de l'entreprise et aux différentes ressources disponibles selon les droits utilisateurs (fichiers partagés, contenus Web, protocoles Telnet, SSH, pilotage distant VNC…).

L'accès à ce service s'effectue depuis une page web où l'utilisateur est invité à saisir ses identifiants. *« Ceci n'est certainement pas une ressource à laquelle vous voulez laisser un attaquant accéder*, rapporte Steven Adair, fondateur de Volexity. *Malheureusement, Volexity a constaté que plusieurs organisations sont des victimes silencieuses de cette page de connexion. »* Selon le chercheur, les attaquants ont réussi à modifier la page de connexion en question en y injectant un code JavaScript. Autrement dit, une backdoor qui *« leur permet de voler subrepticement l'identité des employés pour accéder aux ressources internes de l'entreprise »*.

Deux méthodes d'attaque

Comment s'y prennent les assaillants pour injecter du code dans la page de connexion ? Par deux méthodes, suggère Volexity. La première s'appuie sur l'exploitation de la vulnérabilité CVE-2014-3393 datant d'octobre 2014 et affectant le portail Cisco Clientless SSL VPN. Une faille que Cisco avait corrigée dans la foulée de sa publication, mais qui persiste. Volexity l'a ainsi retrouvée dans nombre de sites d'organisations non gouvernementales dans les secteurs de la santé, des Think Tank, des milieux académiques ainsi que des multinationales de l'électronique et de l'industrie. Aucun nom n'a toutefois été cité.

L'autre vecteur d'attaque *« nécessite une bonne vieille méthode d'accès à l'administration »*. Autrement dit, en obtenant les identifiants de connexion des utilisateurs au service VPN suite à l'installation de keylogger (enregistreur de frappe au clavier), à l'extraction de documents contenant des mots de passe ou à l'exploitation de méthodes de social engineering. *« Volexity sait que c'est possible à 100% et présume que, dans certains cas, les assaillants ont obtenu les accès d'administration à une appliance Cisco ASA dans le but de modifier la page de connexion*, indique la société de sécurité. *Cela peut se faire via le Cisco Adaptive Security Device Manager (AMPS), une interface d'administration Java pour les pare-feu Cisco qui peut être accessible via un navigateur Web. »*

L'erreur est humaine

Il semble donc que cette nouvelle campagne d'infections touchant le service Web VPN de Cisco soit avant tout le fait d'erreurs humaines plus que de véritables défaillances des produits ou le fruit d'une négligence du constructeur. Informé des travaux de Volexity, Cisco invite notamment ses clients à appliquer ses recommandations en matière de protection du réseau.

Le mois dernier, c'est aussi par l'obtention d'identifiants de connexion que nombre de routeurs avaient été victimes de SYNful Knock, un faux firmware à la solde des assaillants et difficile à déloger.

Lire également

Des hackers iraniens derrière de faux profils LinkedIn
Sécurité : des chercheurs de Cisco ralentissent le kit Angler
XOR DDoS : une attaque massive générée par un botnet… Linux

crédit photo © Gajus- shutterstock